25X1

DCI Director of Central Intelligence

HOSTILE EXPLOITATION OF US COMMUNICATIONS AND RELATED AUTOMATED SYSTEMS: A COLLECTION SUPPORT BRIEF (U)

Prepared for the HUMINT Committee by the National Security Agency

Secret

C-JT4-40589
May 1984

Approved For Release 2009/06/30 : CIA-RDP89B01354R000100170083-2

25X1

HOSTILE EXPLOITATION OF US COMMUNICATIONS AND RELATED AUTOMATED SYSTEMS:

A COLLECTION SUPPORT BRIEF (U)

This report was approved by the HUMINT Committee on 2 May 1984.

Approved For Release 2009/06/30 : CIA-RDP89B01354R000100170083-2

25X1

ANNEX C
Glossary

This Annex is a mini-glossary of terms common to COMSEC that the field HUMINT operative might not be familiar with. (U)

1. Automated Systems—The full range of computers, data bases, and automated controls from international networks to individual communications sets and including integrated processing equipment such as communications switches and encryption devices.

2. AUTOSEC—(Automation Security)—The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in an automated system, as well as measures designed to prevent denial of authorized use of the system.

3. Cognizant Agent—A person who is authorized access to national security or national security-related information and who intentionally makes it available to an unauthorized party.

4. COMINT—(Communications Intelligence)—Intelligence information derived from the collection of foreign communications signals.

5. COMSEC (Communications Security)—Protective measures taken to deny unauthorized persons information derived from telecommunications of the US Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to communications security information materials.

6. Cryptanalysis—The steps and operations performed in converting encrypted and plain text without initial knowledge of the key employed in the encryption. In COMSEC, its purpose is to evaluate the adequacy of the security protection that it is intended to provide, or to discover weaknesses or vulnerabilities which could be exploited to defeat or lessen that protection.

7. Cryptography—-The protection of telecommunications by rendering information unintelligible or unrecognizable until it reaches the intended recipient. Also, the design and use of cryptosystems.

8. Cryptovariable—A random appearing sequence used to initially set up and periodically change permutations in cryptoequipment for purposes of encrypting or decrypting electronic signals.

9. ELINT—(Electronic Intelligence)—Intelligence information derived from the collection of foreign noncommunications, electromagnetic radiations emanating from nonnuclear sources.

10. FISINT—(Foreign Instrumentation Signals Intelligence)—Technical intelligence information derived from the intercept of foreign instrumentation signals. These are electromagnetic emissions associated with the testing and operational deployment of non-US

aerospace, surface, and subsurface systems which may have either military or civilian appplication. It includes, but is not limited to, the signals of telemetry, beaconry, electronic interrogators, tracking/fusing/arming/command systems, and video data links. FISINT replaces the older TELINT.

11. IMINT—(Imagery Intelligence)—The collected products of imagery interpretation processed for intelligence use.

12. OPSEC—(Operations Security)—The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

13. SIGINT—(Signals Intelligence)—Intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

14. TEMPEST—The word TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are defined as unintentional data related or intelligence bearing signals which, if intercepted and analyzed, disclose the classified information transmitted, received, handled, or otherwise processed by any information processing equipment. These emanations may be divided into two basic types: electromagnetic and acoustic. Electromagnetic emanations consist of space radiations, stray magnetic fields, conducted signals, and power line modulation. Acoustic emanations consist of sound waves produced by mechanical motions and striking of parts in a functional relationship to the information being processed.

15. TRANSEC (Transmission Security)—The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

16. TSCM—(Technical Security Countermeasures)—A thorough physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and related physical security weaknesses.